AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

An iPhone 8 Plus, Model# MQ8D2LL/A, Serial#C39WK45QJCLY, IMEI#356117090046089, stored at HSI Galveston, Galveston, Texas

Case No. G-18-118

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 8 USC, Section 1324(a)(1)(A)(v)(I); 1324(a)(1)(A)(ii) and 1324(a)(1)(B)(i)	transporting, concealing, harboring, and shielding from detection illegal, in any place, including any building, for the purpose of commercial advantage and private financial gain and the conspiracy thereof

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Santiago Luna, Jr., Special Agent, HSI Galveston
Printed name and title

Sworn to before me and signed in my presence.

Date: 12-6-18

Judge's signature

City and state: Galveston, Texas

Honorable Andrew M. Edison U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF AN IPHONE 8 PLUS, MODEL# MQ8D2LL/A, SERIAL#C39WK45QJCLY, IMEI#356117090046089, STORED AT HSI GALVESTON, 601 ROSENBERG, SUITE 201, GALVESTON, TEXAS	Case No. G-18-118

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **SANTIAGO LUNA, JR.,** being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. My name is Santiago Luna, Jr., and I am a Special Agent employed by the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been employed as a Special Agent since September 1998. I have conducted multiple criminal investigations involving the seizure and examination of electronic devices, including but not limited to computers, cellphones, tablets, and GPS devices. I have conducted multiple criminal investigations for multiple violations of Federal and state laws including, but not limited to alien smuggling and trafficking, marriage, document, and citizenship fraud, narcotics and weapons trafficking, child pornography, and organized criminal activity, to include public corruption. Prior to becoming a Special Agent, I

was employed as a U.S. Border Patrol Trainee for about five months at the U.S. Border Patrol Training Academy in Charleston, South Carolina. Prior to that, I was employed as a Reserve Police Officer for the Rancho Viejo Police Department in Rancho Viejo, Texas, as a patrolman, for almost three years. Before that time, I was employed by the Texas Department of Public Safety, main Headquarters in Austin, Texas, as a security guard for almost three years. I also served previously in the United States Air Force from 1985 to 1989, as an Administrative/Personnel Specialist. As for educational background: I received a Bachelor of Science Degree in Criminal Justice with a minor in Spanish, from Southwest Texas State University (now known as Texas State University), San Marcos, Texas, in 1995.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone 8 Plus, model number MQ8D2LL/A, serial number C39WK45QJCLY, IMEI#356117090046089 (her 'personal' cellular phone) currently stored at HSI Galveston, 601 Rosenberg, Suite 201, Galveston, Texas, seized from Krystal Lynn DIAZ DE LEON-Scurry in Galveston, Texas on November 29, 2018, hereinafter the "Device."

5. The applied-for warrant would authorize the forensic examination of the said Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On November 29, 2018, the Device was seized from Krystal Lynn DIAZ DE LEON-Scurry during her arrest in Galveston, Texas, pursuant to a federal arrest warrant obtained after a true billed Federal Grand Jury indictment was returned for violation of Title 8, United States Code, Sections 1324(a)(1)(A)(v)(I); 1324(a)(1)(A)(ii) and 1324(a)(1)(B)(i), for transporting, concealing, harboring, and shielding from detection illegal, in any place, including any building, for the purpose of commercial advantage and private financial gain and the conspiracy thereof. Through the course of this alien smuggling investigation which also involved an undercover operation, DIAZ DE LEON was observed and confirmed to have recruited, planned, coordinated and facilitated the smuggling of three illegal aliens from the McAllen/Edinburg, Texas area to a pre-planned delivery point in Houston, Texas. Unbeknownst to her, DIAZ DE LEON directly coordinated and voluntarily revealed her alien smuggling plan to a Brazoria County Narcotics Task Force (BCNTF) Investigator, working in an undercover capacity. In her conversations, DIAZ DE LEON revealed that she coordinated, in tandem, with her alien smuggling organization (ASO) 'handlers' in the McAllen/Edinburg area—they provide(d) the illegal aliens to her recruited 'driver(s).' It was noted that she used two cellular phones, interchangeably: Her 'personal' cellular phone with the number of (281) 607-3125, also known as the Device, and her 'business' cellular phone with the number of (281) 603-5114. DIAZ DE LEON used her Device to plan, coordinate and issued specific instructions to the BCNTF undercover Investigator to pick up three illegal aliens in the McAllen/Edinburg area and bring them to Houston; this 'pick-up' occurred as an undercover operation in the form of a controlled delivery of said illegal aliens in early August 2018, with HSI Galveston leading the investigation/operation. She used her Device to successfully lead the 'previously-recruited'

BCNTF undercover investigator to the pickup point as dictated to her by her ASO 'handler.' Not only did DIAZ DE LEON direct and keep in constant communication with the BCNTF undercover Investigator as to the pickup point of the illegal aliens, but she also gave him instructions as to where to deliver them—she communicated this using her Device. She also mentioned about how much she was going to pay the undercover officer ($4,500.00 for all of the three illegal aliens) and where, her bank in Houston. DIAZ DE LEON was identified as the leader of a group of co-conspirators (other drivers) by her statements in that she directed other drivers, beside the undercover officer, to transport illegal aliens from McAllen, TX to Houston, TX. Her Device should contain evidence of DIAZ DE LEON's communications with her co-conspirators and members of the ASO operating from the greater McAllen area(s) regarding the transport and harboring of 'in-country' illegal aliens. These communications would include text messages and call logs. Her Device may also reveal (other) unidentified co-conspirators who were directed by DIAZ DE LEON to transport or harbor the illegal aliens. Furthermore, on the day of DIAZ DE LEON's arrest in Galveston, Texas, she voluntarily stated (via her waived rights) that there was a phone number of an individual of investigative interest contained in her Device—she named the identified the individual by name as 'Danny.'

7. The Device is currently in the lawful possession of the HSI Galveston, Texas. As previously mentioned, it came into HSI Galveston's possession in the following way: On November 29, 2018, the Device was seized from Krystal Lynn DIAZ DE LEON-Scurry during her arrest in Galveston, Texas, pursuant to a Federal arrest warrant obtained after a Federal Grand Jury indictment. Shortly after her arrest, DIAZ DE LEON was read her Miranda Warnings in which she understood them. She voluntarily waived her rights and told the Affiant of this Affidavit that the cellular phone number of an individual ('Danny') that is responsible for

the smuggling of aliens was in her Device she had in her possession at the time of her arrest. When asked for consent to search her phone, she stated that she would only reveal 'Danny's' cellular phone number and not the others. She was informed that that is not how it works in terms of transparency. Therefore, while HSI Galveston Special Agents might already have all necessary authority to examine the Device for hidden evidence accumulated by the previous undercover/controlled delivery operation and via this search incident to arrest, for example, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

8. As stated previously, the Device is currently in storage at HSI GALVESTON, 601 ROSENBERG, SUITE 201, GALVESTON, TEXAS. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this Investigation, in substantially the same state as they were when the Device first came into the possession of the HSI Galveston office.

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other

digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication

devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

10. Based on my training, experience, and research and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.apple.com, I know that the Device has capabilities that allow it to serve as **a** wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Santiago Luna, Jr.
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on December 6, 2018:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone 8 Plus, model number MQ8D2LL/A, serial number C39WK45QJCLY, IMEI#356117090046089 (her 'personal' cellular phone) currently stored at HSI Galveston, 601 Rosenberg, Suite 201, Galveston, Texas, seized from Krystal Lynn DIAZ DE LEON-Scurry in Galveston, Texas on November 29, 2018, hereinafter the "Device."

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 8 USC, Section 1324 and involve Krystal Lynn DIAZ DE LEON-Scurry since June 2018, including:

a. DIAZ DE LEON's communications with her co-conspirators regarding the harboring and transport of her illegal alien employees. These communications would include text messages and call logs.

b. Ownership of the device, including iTunes and App Store account information

c. lists of illegal alien employees and related identifying information;

d. communications between DIAZ DE LEON and employment agencies which provided the illegal aliens, including prices for labor, transport, and housing;

e. any information related to sources of illegal aliens (including names, addresses, phone numbers, or any other identifying information);

f. any information recording DIAZ DE LEON's schedule or travel from June 2018 to the present;

g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol addresses to communicate with mail servers, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.